

*Fors*

*Q1*

# A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER THE INTERNET

## FIELD OF THE INVENTION

The present invention relates generally to credit card transactions and specifically to detecting fraud in such credit card transactions when ordering and downloading information over the <sup>Internet</sup>.

5 *a*

## BACKGROUND OF THE INVENTION

Credit card transactions are being utilized in a variety of environments. In a typical environment a user provides a merchant with a credit card, and the merchant through various means will verify whether that information is accurate. For example, referring now to Figure 1, a typical credit card verification system 10 is shown. In such a system, a merchant 12 receives a credit card from the customer 14. The merchant then verifies the credit card information through an automated <sup>AVS</sup> verification system 16.

15

These systems work well in a credit card transaction in which either the customer has a face-to-face meeting with the merchant or the merchant is actually shipping a package or the like to the address of a customer. The verification procedure typically includes <sup>Receiving at</sup> in the AVS system address information and identity information. However, when downloading information from an online service or the <sup>are</sup> *Internet*, the address and identity information is not enough for to adequately verify that the customer who is purchasing the goods is actually the owner of the credit card. For example, an individual may have both the name and the address of a

20 *a*

particular credit card holder and that information in a normal transaction may be sufficient for authorization of such a transaction. However, <sup>in</sup> ~~as an~~ <sup>Internet</sup> transaction it is possible to <sup>obtain</sup> ~~have~~ all the correct information related to the particular credit card holder through unscrupulous means, and therefore, be able to fraudulently obtain information.

Accordingly, what is needed is a system and method that overcomes the problems associated with a typical verification <sup>system</sup> ~~systems~~ for credit card transactions particularly in the <sup>Internet</sup> ~~internet~~ or online services environment. The system should be easily implemented within the existing environment and should also be straightforwardly applied to existing technology. The present invention addresses such a need.

## SUMMARY

A method and system for detecting fraud in a credit card transaction between a consumer and a merchant over the <sup>Internet</sup> ~~internet~~. The method and system comprises obtaining credit card information relating to the transaction from the consumer; and verifying the credit card information based upon a variety of parameters. The variety of parameters are weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent. In so doing, an integrated verification system is provided which allows a merchant, or the like, to accurately and efficiently determine the validity of a transaction over the <sup>Internet</sup> ~~internet~~.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is diagram of the prior art verification system for credit card transaction.

Figure 2 is a verification system in accordance with the present invention.

5 Figure 3 is a flow chart of the verification system in accordance with the present invention.

Figure 4 is a flow chart of the integrated verification system in accordance with the present invention.

## DETAILED DESCRIPTION

10 The present invention relates to a fraud detection method, system and apparatus for use in credit card transaction over online services or the <sup>Internet</sup> ~~internet~~. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

20 The present invention provides an integrated verification system for credit card transactions over an online service or the <sup>Internet</sup> ~~internet~~. Referring now to Figure 2, what is shown is a block diagram of a system 100 which would use the verification procedure in accordance with the present invention. System 100 includes, similar to

Figure 1, a customer 102 and a merchant 104. The customer 102 provides the merchant with a credit card, and the merchant then sends information from the "IVS" system IVS-106 which includes a variety of parameters providing consistency, history and other information in an integrated fashion to determine whether information is valid. The IVS 106 is typically implemented in software for example in a hard disk, floppy disk or other computer-readable medium. In a typical embodiment, when the customer 102 orders a particular piece of software to be downloaded from a merchant 104, the merchant will provide the credit card number, e-mail address and other pertinent information to the IVS 106. The integrated verification system 106 then weights the variety of parameters so as to provide a merchant with a quantifiable indication on whether the credit and transaction is fraudulent. To more clearly describe the operation of a system and method in accordance with the present invention, refer now to the following discussion in conjunction with the accompanying figures.

Figure 3 shows a simple block diagram for providing an integrated verification of a credit card transaction over the Internet. The IVS 106 includes a controller 212 which receives the credit information from the merchant and then sends that information on to a variety of parameters 202-208. The plurality of parameters that operate on the information to provide an indication of whether the transaction is valid. In this embodiment, the plurality of parameters comprises a history check 202, a consistency check 204, an automatic verification system 206 and an Internet identification verification system 208. The output or individual indications of validity of these parameters are provided to fraud detector 210. The fraud detector 210

combines these inputs to provide an integrated indication of whether the particular transaction is valid.

Consistency check 204 allows <sup>AVS 106</sup> one to determine whether the credit information is consistent, i.e., does the credit information match the user and other information. AVS system 206 provides similar information as AVS 16 described in Figure 1. A key feature of both the history database <sup>222</sup> and the <sup>Internet</sup> ID database <sup>224</sup> is that they can be accessed and the information there within can be supplemented by a variety of other merchants and, therefore, information from those merchants is obtainable thereby.

History information check 202 is provided which also accesses a <sup>history</sup> database 222 which may include card number and email information. The history check 202 will also actively determine if the particular transaction matches previous database information within the history database 222. Therefore, the <sup>Internet</sup> ID verification system <sup>208</sup> and history check <sup>202</sup> increases in utility over time. The <sup>Internet</sup> ID verification system 208 provides for a system for verifying the validity of an <sup>Internet</sup> address, the details of which will be discussed hereinafter. The <sup>Internet</sup> identification verification system <sup>208</sup> similar to the history check <sup>202</sup> includes a database 224 which can be added to by other merchants.

In addition, the <sup>Internet</sup> identification verification system 208 accesses and communicates with a database of <sup>Internet</sup> addresses. This system will be used to verify whether the <sup>Internet</sup> address is consistent with other <sup>Internet</sup> addresses being used in transactions utilizing this credit card.

These different parameters are weighted via weighting blocks 214-220,

respectively, dependent upon the particular credit card transaction. For example, if the amount of dollar transaction is critical, it may be appropriate for the history and check <sup>202</sup> 202

AVS system <sup>206</sup> 202 and 204 to be weighted more critically than the other parameters.

On the other hand, if a critical point is the consistency of the <sup>Internet</sup> <sup>1</sup> internet address, then the consistency check 204 and the <sup>Internet</sup> <sup>1</sup> internet identification system 208 may be more critical. Accordingly, each of the verification parameters 202-208 may be weighted in different amounts depending upon its importance in the verification process.]

A particularly important feature of the present invention is the <sup>Internet</sup> <sup>1</sup> internet identification system 208 and its operation within the integrated verification system 106. Through this system 208, it is possible to quickly determine if an <sup>Internet</sup> <sup>1</sup> internet identification address is being utilized fraudulently. To describe this feature in more detail, refer now to Figure 4 and the accompanying discussion.

Figure 4 is a flow chart of the <sup>Internet</sup> <sup>1</sup> internet identification verification system 208. The goal of <sup>Internet</sup> <sup>1</sup> internet identification verification system 208 is to determine whether the physical address or the physical location of the address compares to a previous physical location that was used for that particular <sup>Internet</sup> <sup>1</sup> internet address. Accordingly, in the flow chart of Figure 4, first the number of transactions that had been processed using that particular <sup>Internet</sup> <sup>1</sup> internet address is obtained from the database 224, via step 302. Thereafter, a map of those transactions is constructed based on those obtained transactions, via step 304. Finally, the constructed map is used to determine if the new credit card transaction is valid, via step 306. Accordingly, through a system and method in accordance with this system, an <sup>Internet</sup> <sup>1</sup> internet identification verification system is provided which can quickly and easily determine whether a particular <sup>Internet</sup> <sup>1</sup> internet

A  
address is related to a particular credit <sup>card</sup> ~~care~~ transaction.

Accordingly, what is provided is a system and method for accurately determining whether a particular credit card transaction is a fraudulent one. The integrated verification system in accordance with the present invention provides for weighting the variety of parameters so as to provide a merchant with a quantifiable indication on whether the credit and transaction is fraudulent.

5  
10  
15  
Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will recognize that there could be variations to the embodiment and those variations would be within the spirit and scope of the present invention. Therefore, although the present invention was described in terms of a particular verification system, one of ordinary skill in the art readily recognizes, that any number of parameters can be utilized and their use would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill without departing from the spirit and scope of the present invention, the scope of which is defined by the following claims.